REV - flappy bird - Easy

> Whiterose is wary of you and the pride you take in stopping unethical hacks. Gift them a cracked flappy bird game to raise confusion regarding your morals and buy yourself some time.

In the executable file, we see lines indicating that the source code was written in Python.

```
Installing PYZ: Could not get sys.path
import sys; sys.stdout.flush();          (sys.__stdout__.flush if sys.__stdout__          is not sys.stdout else (lambda: None))()
import sys; sys.stderr.flush();          (sys.__stderr__.flush if sys.__stderr__          is not sys.stderr else (lambda: None))()
```

Let's try to get PYZ files. PYZ is a Python file placed in a Zip archive. Pyinstxtractor displays a warning that some files cannot be retrieved because Python version 3.10 is required.

```
└─$ python3 pyinstxtractor.py ../flappy_birb
[+] Processing ../flappy_birb
[+] Pyinstaller version: 2.1+
[+] Python version: 3.10
[+] Length of package: 16189512 bytes
[+] Found 122 files in CArchive
[+] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap.pyc
[+] Possible entry point: pyi_rth_inspect.pyc
[+] Possible entry point: pyi_rth_pkgres.pyc
[+] Possible entry point: pyi_rth_pkgutil.pyc
[+] Possible entry point: main.pyc
[!] Warning: This script is running in a different Python version than the one used to build the executable.
[!] Please run this script in Python 3.10 to prevent extraction errors during unmarshalling
[!] Skipping pyz extraction
[+] Successfully extracted pyinstaller archive: ../flappy_birb

You can now use a python decompiler on the pyc files within the extracted directory
```

By installing Python 3.10 we get all the PYC files. Using pycdc we get the source file main.py. Among the imported libraries we see the license_check imported from the license_key file.

```
import pygame
import sys
import random
import time
from license_key import license_check
```

The file license_key.py stores the encrypted flag, using the same encryption algorithm we get the original flag!

```
import sys

def custom_encode(data):
    encoded_data = ''
    for char in data:
        if char.isalpha():
            if char.isupper():
                encoded_char = chr(((ord(char) - 65) + 13) % 26 + 65)
            else:
                encoded_char = chr(((ord(char) - 97) + 13) % 26 + 97)
        else:
            encoded_char = char
        encoded_data += encoded_char
    return encoded_data


def custom_decode(encoded_data):
    return custom_encode(encoded_data)


def license_check(user_input_key):
    if user_input_key ==
custom_decode('PUPGS{JU3A_J3_1053_0He_Ce1AP1C135_J3_1AI173_PU405}'):
        print('Premium Content Unl0cked!!!')
    else:
        print('Sorry license check failed. Please enter valid key.')
    sys.exit()
```

> Flag: **CHCTF{WH3N_W3_1053_0Ur_Pr1NC1P135_W3_1NV173_CH405}**